CLAIMS

What is claimed is:

1   1.   A method of dynamically mitigating a noncompliant password, the method
2   comprising the machine-implemented steps of:
3   obtaining a password from a user when the user attempts to access a service;
4   determining whether the password meets quality criteria; and
5   if the password does not meet the quality criteria, performing one or more responsive
6   actions that relate to accessing the service.

1   2.   The method of Claim 1, wherein the step of performing one or more responsive
2   actions that relate to accessing the service comprises:
3   if the password meets the quality criteria, granting to the user a first level of access to
4   the service, wherein the first level of access to the service is associated with
5   the quality criteria;
6   if the password meets a second quality criteria, granting to the user a second level of
7   access to the service, wherein the second level of access to the service is
8   associated with the second quality criteria, wherein the second quality criteria
9   is distinct from the quality criteria and wherein, if a particular password meets
10   the quality criteria, then the password meets the second quality criteria.

1   3.   The method of Claim 1, wherein the step of performing one or more responsive
2   actions that relate to accessing the service comprises performing one or more of:
3   logging information related to the password;
4   sending a report about the password;
5   generating an alert about the password;
6   forcing a password change; or
7   blocking the user's access to the service.

1   4.   The method of Claim 1, wherein the method further comprises, if the password does
2   meet the quality criteria, providing user access to the service.

1   5.   The method of Claim 1,,wherein the step of determining whether the password meets
2   quality criteria further comprises one or more of the steps of:
3   performing a dictionary look-up based on the one or more symbols used in the
4   password;
5   checking the length of the one or more symbols used in the password;
6   checking the number of unique characters of the one or more symbols used in the
7   password;
8   checking the case of the characters in the one or more symbols used in the password;
9   checking the sequencing of characters in the one or more symbols used in the
10   password; or
11   performing statistical analysis based on the one or more symbols used in the
12   password.

1   6.   The method of Claim 1, wherein the step of performing one or more responsive
2   actions that relate to accessing the service comprises logging information related to the
3   password.

1   7.   The method of Claim 1, wherein the step of performing one or more responsive
2   actions that relate to accessing the service comprises sending a report about the password.

1   8.   The method of Claim 1, wherein the step of performing one or more responsive
2   actions that relate to accessing the service comprises generating an alert about the password.

1   9.   The method of Claim 1, wherein the step of performing one or more responsive
2   actions that relate to accessing the service comprises forcing a password change.

1   10.   The method of Claim 1, wherein the step of performing one or more responsive
2   actions that relate to accessing the service comprises blocking the user's access to the
3   service.

1   11.   The method of Claim 1, wherein obtaining the password from the user comprises
2   obtaining the password from the user via a graphical user interface.

1   12.   The method of Claim 1, wherein obtaining the password from the user comprises
2   obtaining the password from the user via an electronic interface.

1   13.   The method of Claim 1, wherein the method further comprises the step of
2   determining a quality score for the password, and wherein the step of determining whether
3   the password meets quality criteria comprises comparing the quality score to a predefined
4   threshold value.

1   14.   The method of Claim 1, further comprising the steps of:
2   obtaining the password from a repository of passwords;
3   making a first determination whether the password meets quality criteria; and
4   storing in a particular machine-readable medium an indication of the first
5   determination for the password;
6   wherein the step of determining whether the password meets quality criteria
7   comprises accessing the particular machine-readable medium.

1   15.   The method of Claim 1, wherein the user is associated with a particular user role, and
2   wherein determining whether the password meets quality criteria comprises determining
3   whether the password meets quality criteria for the particular user role.

1   16.   The method of Claim 1, wherein determining whether the password meets quality
2   criteria comprises determining whether the password meets quality criteria for the service.

1   17.   The method of Claim 1, wherein the step of obtaining the password comprises an

2   access service obtaining the password from the user when the user attempts to access the

3   service, and wherein the access service comprises machine executable instructions executing

4   on a particular machine, and the service comprises machine executable instruction executing

5   on the same particular machine.

1   18.   The method of Claim 1, wherein the step of obtaining the password comprises an

2   access service obtaining the password from the user when the user attempts to access the

3   service, and wherein the access service comprises machine executable instructions executing

4   on a first machine and the service comprises machine executable instructions executing on a

5   second machine, wherein the first machine is distinct from the second machine.

1   19.   A method of dynamically mitigating a noncompliant password, the method

2   comprising the machine-implemented steps of:

3   obtaining a password from a user when the user attempts to access a service;

4   determining whether the password meets quality criteria; and

5   if the password does not meet the quality criteria, performing one or more of:

6   forcing a password change; or

7   blocking the user's access to the service; and

8   wherein the step of determining whether the password meets quality criteria further

9   comprises one or more of the steps of:

10   performing a dictionary look-up based on the one or more symbols used in the

11   password;

12   checking the length of the one or more symbols used in the password;

13   checking the number of unique characters of the one or more symbols used in

14   the password;

15   checking the case of the characters in the one or more symbols used in the

16   password;

17   checking the sequencing of characters in the one or more symbols used in the

18   password; or

19   performing statistical analysis based on the one or more symbols used in the

20   password.

1   20.   A machine-readable medium carrying one or more sequences of instructions for

2   dynamically mitigating a noncompliant password, which instructions, when executed by one

3   or more processors, cause the one or more processors to carry out the steps of:

4   obtaining a password from a user when the user attempts to access a service;

5   determining whether the password meets quality criteria; and

6   if the password does not meet the quality criteria, performing one or more responsive

7   actions that relate to accessing the service.

1   21.   The machine-readable medium of Claim 20, wherein the step of performing one or

2   more responsive actions that relate to accessing the service comprises:

3   if the password meets the quality criteria, granting to the user a first level of access to

4   the service, wherein the first level of access to the service is associated with

5   the quality criteria;

6   if the password meets a second quality criteria, granting to the user a second level of

7   access to the service, wherein the second level of access to the service is

8   associated with the second quality criteria, wherein the second quality criteria

9   is distinct from the quality criteria and wherein, if a particular password meets

10   the quality criteria, then the password meets the second quality criteria.

1   22.   The machine-readable medium of Claim 20, wherein the step of performing one or

2   more responsive actions that relate to accessing the service comprises performing one or

3   more of:

4   logging information related to the password;

5   sending a report about the password;

6   generating an alert about the password;

7   forcing a password change; or

8   blocking the user's access to the service.

1   23.   The machine-readable medium of Claim 20, further comprising instructions which,
2   when executed by the one or more processors, cause the one or more processors to carry out
3   the step of, if the password does meet the quality criteria, providing user access to the
4   service.

1   24.   The machine-readable medium of Claim 20, wherein the step of determining whether
2   the password meets quality criteria further comprises one or more of the steps of:
3   performing a dictionary look-up based on the one or more symbols used in the
4   password;
5   checking the length of the one or more symbols used in the password;
6   checking the number of unique characters of the one or more symbols used in the
7   password;
8   checking the case of the characters in the one or more symbols used in the password;
9   checking the sequencing of characters in the one or more symbols used in the
10   password; or
11   performing statistical analysis based on the one or more symbols used in the
12   password.

1   25.   The machine-readable medium of Claim 20, wherein the step of performing one or
2   more responsive actions that relate to accessing the service comprises logging information
3   related to the password.

1   26.   The machine-readable medium of Claim 20, wherein the step of performing one or
2   more responsive actions that relate to accessing the service comprises sending a report about
3   the password.

1   27.   The machine-readable medium of Claim 20, wherein the step of performing one or
2   more responsive actions that relate to accessing the service comprises generating an alert
3   about the password.

1   28.   The machine-readable medium of Claim 20, wherein the step of performing one or

2   more responsive actions that relate to accessing the service comprises forcing a password

3   change.

1   29.   The machine-readable medium of Claim 20, wherein the step of performing one or

2   more responsive actions that relate to accessing the service comprises blocking the user's

3   access to the service.

1   30.   The machine-readable medium of Claim 20, wherein obtaining the password from the

2   user comprises obtaining the password from the user via a graphical user interface.

1   31.   The machine-readable medium of Claim 20, wherein obtaining the password from the

2   user comprises obtaining the password from the user via an electronic interface.

1   32.   The machine-readable medium of Claim 20, further comprising instructions which,

2   when executed by the one or more processors, cause the one or more processors to carry out

3   the step of determining a quality score for the password, and wherein the step of determining

4   whether the password meets quality criteria comprises comparing the quality score to a

5   predefined threshold value.

1   33.   The machine-readable medium of Claim 20, further comprising instructions which,

2   when executed by the one or more processors, cause the one or more processors to carry out

3   the steps of:

4   obtaining the password from a repository of passwords;

5   making a first determination whether the password meets quality criteria; and

6   storing in a particular machine-readable medium an indication of the first

7   determination for the password;

8   and wherein the step of determining whether the password meets quality criteria

9   comprises accessing the particular machine-readable medium.

1   34.   The machine-readable medium of Claim 20, wherein the user is associated with a

2   particular user role, and wherein determining whether the password meets quality criteria

3   comprises determining whether the password meets quality criteria for the particular user

4   role.

1   35.   The machine-readable medium of Claim 20, wherein determining whether the

2   password meets quality criteria comprises determining whether the password meets quality

3   criteria for the service.

1   36.   An apparatus for dynamically mitigating a noncompliant password, comprising:

2   means for obtaining a password from a user when the user attempts to access a

3   service;

4   means for determining whether the password meets quality criteria; and

5   means for performing one or more responsive actions that relate to accessing the

6   service if the password does not meet the quality criteria.

1   37.   The apparatus of Claim 36, wherein the means for performing one or more responsive

2   actions that relate to accessing the service comprises:

3   means for granting to the user a first level of access to the service, if the password

4   meets the quality criteria, wherein the first level of access to the service is

5   associated with the quality criteria;

6   means for granting to the user a second level of access to the service, if the password

7   meets a second quality criteria, wherein the second level of access to the

8   service is associated with the second quality criteria, wherein the second

9   quality criteria is distinct from the quality criteria and wherein, if a particular

10   password meets the quality criteria, then the password meets the second

11   quality criteria..

1   38.   The apparatus of Claim 36, wherein the means for performing one or more responsive

2   actions that relate to accessing the service comprises one or more of:

3   means for logging information related to the password;

4   means for sending a report about the password;

5   means for generating an alert about the password;

6   means for forcing a password change; or

7   means for blocking the user's access to the service.

1   39.   The apparatus of Claim 36, wherein the apparatus further comprises means for

2   providing user access to the service if the password does meet the quality criteria.

1   40.   The apparatus of Claim 36, wherein the means for determining whether the password

2   meets quality criteria further comprises one or more of:

3   means for performing a dictionary look-up based on the one or more symbols used in

4   the password;

5   means for checking the length of the one or more symbols used in the password;

6   means for checking the number of unique characters of the one or more symbols used

7   in the password;

8   means for checking the case of the characters in the one or more symbols used in the

9   password;

10   means for checking the sequencing of characters in the one or more symbols used in

11   the password; or

12   means for performing statistical analysis based on the one or more symbols used in

13   the password.

1   41.   The apparatus of Claim 36, wherein the means for performing one or more responsive

2   actions that relate to accessing the service comprises means for logging information related

3   to the password.

1   42.   The apparatus of Claim 36, wherein the means for performing one or more responsive
2   actions that relate to accessing the service comprises means for sending a report about the
3   password.

1   43.   The apparatus of Claim 36, wherein the means for performing one or more responsive
2   actions that relate to accessing the service comprises means for generating an alert about the
3   password.

1   44.   The apparatus of Claim 36, wherein the means for performing one or more responsive
2   actions that relate to accessing the service comprises means for forcing a password change.

1   45.   The apparatus of Claim 36, wherein the means for performing one or more responsive
2   actions that relate to accessing the service comprises means for blocking the user's access to
3   the service.

1   46.   The apparatus of Claim 36, wherein the means for obtaining the password from the
2   user comprises means for obtaining the password from the user via a graphical user interface.

1   47.   The apparatus of Claim 36, wherein the means for obtaining the password from the
2   user comprises means for obtaining the password from the user via an electronic interface.

1   48.   The apparatus of Claim 36, wherein the apparatus further comprises means for
2   determining a quality score for the password, and wherein the means for determining whether
3   the password meets quality criteria comprises means for comparing the quality score to a
4   predefined threshold value.

1   49.   The apparatus of Claim 36, further comprising:
2   means for obtaining the password from a repository of passwords;

3   means for making a first determination whether the password meets quality
4   criteria; and
5   means for storing in a particular machine-readable medium an indication of
6   the first determination for the password;
7   and wherein the means for determining whether the password meets quality criteria
8   comprises means for accessing the particular machine-readable medium.

1   50.   The apparatus of Claim 36, wherein the user is associated with a particular user role,
2   and wherein means for determining whether the password meets quality criteria comprises
3   means for determining whether the password meets quality criteria for the particular user
4   role.

1   51.   The apparatus of Claim 36, wherein means for determining whether the password
2   meets quality criteria comprises means for determining whether the password meets quality
3   criteria for the service.

1   52.   The apparatus of Claim 36, wherein the means for obtaining the password comprises
2   means for an access service to obtain the password from the user when the user attempts to
3   access the service, and wherein the access service comprises means for executing on a
4   particular machine, and wherein the service comprises means for executing on the same
5   particular machine.

1   53.   The apparatus of Claim 36, wherein the means for obtaining the password comprises
2   means for an access service to obtain the password from the user when the user attempts to
3   access the service, and wherein the access service comprises means for executing on a first
4   machine and the service comprises means for executing on a second machine, wherein the
5   first machine is distinct from the second machine.

1   54.   An apparatus for dynamically mitigating a noncompliant password, comprising:

2   a network interface that is coupled to the data network for receiving one or more packet

3   flows therefrom;

4   a processor;

5   one or more stored sequences of instructions which, when executed by the processor, cause

6   the processor to carry out the steps of:

7   obtaining a password from a user when the user attempts to access a service;

8   determining whether the password meets quality criteria; and

9   if the password does not meet the quality criteria, performing one or more responsive

10   actions that relate to accessing the service.

1   55.   The apparatus of Claim 54, wherein the step of performing one or more responsive

2   actions that relate to accessing the service comprises:

3   if the password meets the quality criteria, granting to the user a first level of access to

4   the service, wherein the first level of access to the service is associated with

5   the quality criteria;

6   if the password meets a second quality criteria, granting to the user a second level of

7   access to the service, wherein the second level of access to the service is

8   associated with the second quality criteria, wherein the second quality criteria

9   is distinct from the quality criteria and wherein, if a particular password meets

10   the quality criteria, then the password meets the second quality criteria.

1   56.   The apparatus of Claim 54, wherein the step of performing one or more responsive

2   actions that relate to accessing the service comprises performing one or more of:

3   logging information related to the password;

4   sending a report about the password;

5   generating an alert about the password;

6   forcing a password change; or

7   blocking the user's access to the service.

1   57.   The apparatus of Claim 54, wherein the apparatus further comprises one or more

2   stored sequences of instructions which, when executed by the processor, cause the processor

3   to carry out the step of, if the password does meet the quality criteria, providing user access

4   to the service.

1   58.   The apparatus of Claim 54, wherein the step of determining whether the password

2   meets quality criteria comprises one or more of the steps of:

3   performing a dictionary look-up based on the one or more symbols used in the

4   password;

5   checking the length of the one or more symbols used in the password;

6   checking the number of unique characters of the one or more symbols used in the

7   password;

8   checking the case of the characters in the one or more symbols used in the password;

9   checking the sequencing of characters in the one or more symbols used in the

10   password; or

11   performing statistical analysis based on the one or more symbols used in the

12   password.

1   59.   The apparatus of Claim 54, wherein the step of performing one or more responsive

2   actions that relate to accessing the service comprises logging information related to the

3   password.

1   60.   The apparatus of Claim 54, wherein the step of performing one or more responsive

2   actions that relate to accessing the service comprises sending a report about the password.

1   61.   The apparatus of Claim 54, wherein the step of performing one or more responsive

2   actions that relate to accessing the service comprises generating an alert about the password.

1   62.   The apparatus of Claim 54, wherein the step of performing one or more responsive

2   actions that relate to accessing the service comprises forcing a password change.

1   63.   The apparatus of Claim 54, wherein the step of performing one or more responsive

2   actions that relate to accessing the service comprises blocking the user's access to the

3   service.

1   64.   The apparatus of Claim 54, wherein obtaining the password from the user comprises

2   obtaining the password from the user via a graphical user interface.

1   65.   The apparatus of Claim 54, wherein obtaining the password from the user comprises

2   obtaining the password from the user via an electronic interface.

1   66.   The apparatus of Claim 54, wherein the apparatus further comprises one or more

2   stored sequences of instructions which, when executed by the processor, cause the processor

3   to carry out the step of determining a quality score for the password, and wherein the step of

4   determining whether the password meets quality criteria comprises comparing the quality

5   score to a predefined threshold value.

1   67.   The apparatus of Claim 54, further comprising one or more stored sequences of

2   instructions which, when executed by the processor, cause the processor to carry out the steps

3   of:

4   obtaining the password from a repository of passwords;

5   making a first determination whether the password meets quality criteria; and

6   storing in a particular machine-readable medium an indication of the first

7   determination for the password;

8   and wherein the step of determining whether the password meets quality criteria

9   comprises accessing the particular machine-readable medium.

1 68. The apparatus of Claim 54, wherein the user is associated with a particular user role,

2 and wherein determining whether the password meets quality criteria comprises determining

3 whether the password meets quality criteria for the particular user role.

1 69. The apparatus of Claim 54, wherein determining whether the password meets quality

2 criteria comprises determining whether the password meets quality criteria for the service.

1 70. The apparatus of Claim 54, wherein the step of obtaining the password comprises an

2 access service obtaining the password from the user when the user attempts to access the

3 service, and wherein the access service comprises machine executable instructions executing

4 on the apparatus, and the service comprises machine executable instruction executing on the

5 same apparatus.

1 71. The apparatus of Claim 54, wherein the step of obtaining the password comprises an

2 access service obtaining the password from the user when the user attempts to access the

3 service, and wherein the access service comprises machine executable instructions executing

4 on a first machine and the service comprises machine executable instructions executing on a

5 second machine, wherein the first machine is distinct from the second machine.